

2005 DRAFTING REQUEST

Bill

Received: **02/18/2005**

Received By: **csundber**

Wanted: **As time permits**

Identical to LRB:

For: **Louis Molepske (608) 267-9649**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - electron com**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Molepske@legis.state.wi.us**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Require disclosure to customer if security of data pertaining to customer is breached.

Instructions:

See Attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P1	csundber 03/10/2005 csundber 03/29/2005	jdyer 03/14/2005 jdyer 03/29/2005	jfrantze 03/14/2005	_____	sbasford 03/15/2005		
/1	csundber 07/13/2005	wjackson 07/19/2005	jfrantze 03/29/2005	_____	sbasford 03/29/2005		S&L
/2	csundber 07/22/2005	wjackson 07/25/2005	pgreensl 07/19/2005	_____	sbasford 07/19/2005		State

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/3			rschluet 07/26/2005	_____	lnorthro 07/26/2005	lemery 07/26/2005	State

FE Sent For: 07/26/2005.

<END>

2005 DRAFTING REQUEST

Bill

Received: **02/18/2005**

Received By: **csundber**

Wanted: **As time permits**

Identical to LRB:

For: **Louis Molepske (608) 267-9649**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - electron com**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Molepske@legis.state.wi.us**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Require disclosure to customer if security of data pertaining to customer is breached.

Instructions:

See Attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P1	csundber 03/10/2005	jdyer 03/14/2005	jfrantze 03/14/2005	_____	sbasford 03/15/2005		
	csundber 03/29/2005	jdyer 03/29/2005		_____			
/1	csundber 07/13/2005	wjackson 07/19/2005	jfrantze 03/29/2005	_____	sbasford 03/29/2005		S&L
/2	csundber 07/22/2005	wjackson 07/25/2005	pgreensl 07/19/2005	_____	sbasford 07/19/2005		State

Vers. Drafted Reviewed Typed Proofed Submitted Jacketed Required

/3 rschluet _____ Inorthro State
07/26/2005 _____ 07/26/2005

FE Sent For:

<END>

"/3" Per
Rep
7/26/05 Molepske

2005 DRAFTING REQUEST

Bill

Received: 02/18/2005

Received By: csundber

Wanted: As time permits

Identical to LRB:

For: Louis Molepske (608) 267-9649

By/Representing:

This file may be shown to any legislator: NO

Drafter: csundber

May Contact:

Addl. Drafters:

Subject: Trade Regulation - electron com

Extra Copies:

Submit via email: YES

Requester's email: Rep.Molepske@legis.state.wi.us

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Require disclosure to customer if secuity of data pertaining to customer is breached.

Instructions:

See Attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P1	csundber 03/10/2005 csundber 03/29/2005	jdye 03/14/2005 jdye 03/29/2005	jfrantze 03/14/2005	_____	sbasford 03/15/2005		
/1	csundber 07/13/2005	wjackson 07/19/2005	jfrantze 03/29/2005	_____	sbasford 03/29/2005		S&L
/2		13 wj 7/25	pgreensl 07/19/2005	_____	sbasford 07/19/2005		State

Vers. Drafted Reviewed Typed Proofed Submitted Jacketed Required

FE Sent For:

<END>

2005 DRAFTING REQUEST

Bill

Received: 02/18/2005

Received By: csundber

Wanted: As time permits

Identical to LRB:

For: Louis Molepske (608) 267-9649

By/Representing:

This file may be shown to any legislator: NO

Drafter: csundber

May Contact:

Addl. Drafters:

Subject: Trade Regulation - electron com

Extra Copies:

Submit via email: YES

Requester's email: Rep.Molepske@legis.state.wi.us

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Require disclosure to customer if security of data pertaining to customer is breached.

Instructions:

See Attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P1	csundber 03/10/2005	jdye 03/14/2005	jfrantze 03/14/2005	_____	sbasford 03/15/2005		
	csundber 03/29/2005	jdye 03/29/2005		7/19			
/1		12/17/19	jfrantze 03/29/2005	7/19 P8115	sbasford 03/29/2005		S&L

FE Sent For:

2005 DRAFTING REQUEST

Bill

Received: 02/18/2005

Received By: csundber

Wanted: As time permits

Identical to LRB:

For: Louis Molepske (608) 267-9649

By/Representing:

This file may be shown to any legislator: NO

Drafter: csundber

May Contact:

Addl. Drafters:

Subject: Trade Regulation - electron com

Extra Copies:

Submit via email: YES

Requester's email: Rep.Molepske@legis.state.wi.us

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Require disclosure to customer if secuity of data pertaining to customer is breached.

Instructions:

See Attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P1	csundber 03/10/2005	jdyer 03/14/2005	jfrantze 03/14/2005	_____	sbasford 03/15/2005		

FE Sent For:

1 3
29 JW 83629-76/RS
3 29
<END>

2005 DRAFTING REQUEST

Bill

Received: **02/18/2005**

Received By: **csundber**

Wanted: **As time permits**

Identical to LRB:

For: **Louis Molepske (608) 267-9649**

By/Representing:

This file may be shown to any legislator: **NO**

Drafter: **csundber**

May Contact:

Addl. Drafters:

Subject: **Trade Regulation - electron com**

Extra Copies:

Submit via email: **YES**

Requester's email: **Rep.Molepske@legis.state.wi.us**

Carbon copy (CC:) to:

Pre Topic:

No specific pre topic given

Topic:

Require disclosure to customer if security of data pertaining to customer is breached.

Instructions:

See Attached

Drafting History:

<u>Vers.</u>	<u>Drafted</u>	<u>Reviewed</u>	<u>Typed</u>	<u>Proofed</u>	<u>Submitted</u>	<u>Jacketed</u>	<u>Required</u>
/P1	csundber	P1 3/14 jld	2/15/05	2/15/05			

FE Sent For:

<END>



WISCONSIN STATE REPRESENTATIVE

Louis J. Molepske, Jr.

71ST ASSEMBLY DISTRICT

To: Legislative Reference Bureau, Jeff Kuesel

From: Representative Louis J. Molepske Jr.

Re: Drafting Request—Wisconsin Security Breach Information Act

Date: February 16, 2005

I am requesting a draft for a bill to be entitled the Wisconsin Security Breach Information Act. The bill will mandate that businesses must inform customers when electronic data is compromised by a hacker. I would like to model it after a similar California law.

For your reference I have enclosed a copy of the California law along with a number of articles explaining the practical aim and effect of the bill. Of course, if you have any questions, please do not hesitate to contact me.

Thank you for your assistance.

HOME:
924 Lindbergh Ave
Stevens Point, WI 54481
(715) 342-8985
Rep.Molepske@legis.state.wi.us

www.legis.state.wi.us



STATE CAPITOL:
P.O. Box 8953
Madison, WI 53708-8953
Toll-free: 888-534-0071 or (608)267-9649
FAX: (608) 282-3671

2/23 C. Molepske

Security breaches: add

① Disc. must contain info.
as to how to contact credit
reporting agencies

② Entity whose security was
breached must also alert
3 major credit report firms
that there was breach of
individual's secure data

KB 2696

AB 884



Try Money FREE
Subscribe to Money

QUOTE
SYMBOL LOOK-UP

QUOTE

SEARCH

☒ Web

☐ CNN/Money



[Home](#)

[News](#)

[Markets](#)

[Technology](#)

[Commentary](#)

[Personal Finance](#)

[Autos](#)

NEWS > Technology

[SAVE](#) | [EMAIL](#) | [PRINT](#) | [SUBSCRIBE TO MONEY](#)

Thieves steal consumer info database

Personal info compiled by ChoicePoint stolen, including Social Security numbers; thousands affected.

February 15, 2005: 6:51 PM EST

WASHINGTON (Reuters) - Tens of thousands of U.S. consumers face a greater risk of identity theft after criminals gained access to a database of personal records compiled by ChoicePoint Inc., a company spokesman said Tuesday.

Identity thieves posing as legitimate businesses were able to access profiles that include Social Security numbers, credit histories, criminal records and other sensitive material, ChoicePoint spokesman Chuck Jones said.

Alpharetta, Georgia-based [ChoicePoint \(Research\)](#) maintains personal profiles of nearly every U.S. consumer, which it sells to employers, landlords, marketing companies and about 35 U.S. government agencies.

In California, the only state that requires companies to disclose security breaches, ChoicePoint sent warning letters to 30,000 to 35,000 consumers advising them to check their credit reports.

Jones said the company was still determining whether consumers outside California were affected, and declined to say whether it would notify them.

"We will look at it at that time if we determine that's the case," he said.

Investigators notified the company of the breach in October, but ChoicePoint did not send out the consumer warnings until last week. Jones said it took a while for the company to determine which consumer records were affected.

The identity thieves set up roughly 50 fraudulent business accounts to gain access to consumer data, Jones said. The company has since tightened its criteria for access, he said.

A Postal Service inspector said the agency could not talk about ongoing cases. Other authorities involved in the investigation did not immediately return calls requesting comment.

ChoicePoint's databases contain 19 billion public records, including driving records, sex-offender lists and FBI lists of wanted criminals and suspected terrorists.

The company says its records enable law enforcers to track down serial killers and have helped find 822 missing children.

Privacy concerns

Top Story

[Applied M](#)

[Gains ahe
Greenspa](#)

[Buffett, Sc](#)

[Thieves st
info datab](#)

[Microsoft
browser v](#)

ADVE

ChoicePoint has drawn criticism from privacy activists who say it should face greater limits on how it handles the detailed profiles it has amassed on nearly every U.S. citizen.

Chris Hoofnagle, associate director with the Electronic Privacy Information Center, noted another consumer-data company, Acxiom (Research), suffered a security breach as well. That occurred in 2003.

"This calls into question whether these data products actually make us more secure," he said. "This is a prime example of how they don't and why ChoicePoint should be subject to federal privacy regulations," he said.

In several recent filings with the Federal Trade Commission, Hoofnagle has argued ChoicePoint should be subject to a law that allows consumers to view their credit reports and see who else is accessing them.

People can lose their jobs because of erroneous ChoicePoint records, he said, while predators can too easily tap the database to track down victims.

ChoicePoint said in a December response it complied with existing laws and gave consumers more access to their own files than required.

"The topic of the responsible use of information is a vital one to our society ... we support a national debate on this very topic," ChoicePoint President Doug Curling said. ■

The Hot List

[Hot housing markets](#)

[Best car buys 2005](#)

[Stocks we love](#)

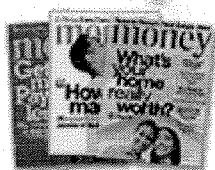
More Technology

[Applied Materials profits soar](#)

[Microsoft plans new browser version](#)

[Survey: Amazon, eBay lose appeals?](#)

money TRY AN ISSUE OF MONEY MAGAZINE FREE



Name

State/Pr

[Privacy Policy](#)

Address

Zip/Postal

City

E-mail

[contact us](#) | [magazine customer service](#) | [site map](#) | [glossary](#) | [RSS](#) | [press room](#)

OTHER NEWS: [CNN](#) | [SI](#) | [Fortune](#) | [Business2.0](#)

» = Money subscribers * = Premium content

Copyright 2005 Reuters All rights reserved. This material may not be published, broadcast, rewritten, or redistributed.

--* Disclaimer

© 2005 Cable News Network LP, LLLP. A Time Warner Company ALL RIGHTS RESERVED.

[Terms](#) under which this service is provided to you. [privacy policy](#) [Reprints](#) of site stories are available.



online
is
click

- Bachelor's Admin in Finance
- Master's Admin in Finance
- Bachelor's Criminal
- Bachelor's Business
- Bachelor's Business Health
- Bachelor's Visual C
- Bachelor's Informal
- Master's Business
- Master's Business Health
- Master's Informal
- Master's Education

CLICK
TO LE

YOUR E-MAIL

Follow the matters to **own** alert t topics you'

Or, visit **Pc** suggestion

Manage ale

Explore the TechTarget Network at SearchTechTarget.com.

Activate your FREE membership



The world's most security specific information resource for enterprise IT professionals



The highest level of SSL encryption available, period.

HOME | NEWS | TOPICS | ITKNOWLEDGE EXCHANGE | TIPS | ASK THE EXPERTS | WEBCASTS | WHITE PAPER

SEARCH this site and the web

SEARCH

ADVANCED SEARCH | SITE MAP

Search Page



Stay secure with the world's most trusted source for unbiased security expertise. Get your free subscription to Information Security today!

Home > News > California scre...

EMAIL THIS

Security News:

Search for:

in

ALL NEWS



SEARCH

Full TargetSearch with Google

California screaming: Companies must disclose security breaches

By Edward Hurley, SearchSecurity.com News Writer
30 Jun 2003 | SearchSecurity.com



California's Security Breach Information Act (SB 1386) becomes official Tuesday and mandates for the first time that businesses must inform customers when electronic data is compromised by a hacker.

SB 1386 requires companies that own or maintain the personal information of California residents to notify the people if that data is unlawfully accessed.

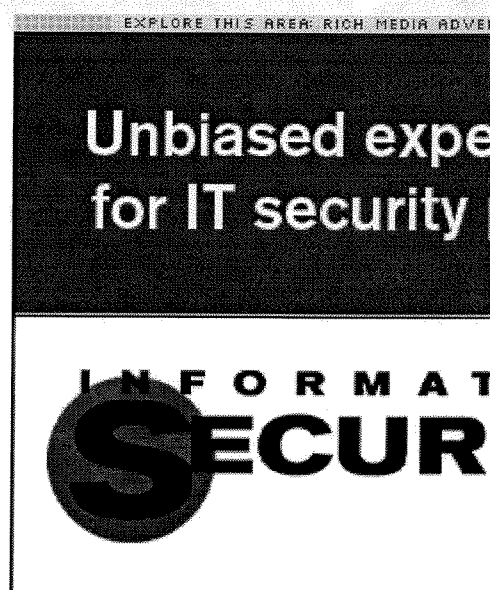
Gray areas remain with SB 1386 -- for example, it's unclear whether the state can impose the law upon companies that operate outside the state but own personal data about California residents.

Some industry opposition has been voiced, which softened the law somewhat while it was being written. But "it issues a mandatory disclosure requirement that, to my knowledge, has not existed in another state or federal law," said Steve Pink, deputy chairman of the American Bar Association's Cybersecurity Task Force and an attorney with Gray Cary Ware & Freidenrich. Pink presented a tutorial last week on SB 1386 that was sponsored by vulnerability scanning outsourcer Qualys Inc.

The impetus for the law was the hacking of a database of state employee information. Sensitive information, such as names, Social Security numbers and payroll information about state employees "ranging from office workers to judges," was stolen, Pink said.

The breach occurred April 5, 2002, but it wasn't discovered until May 7. The state didn't notify the public of it until May 24. The public created a lot of criticism and an outcry, Pink said. The California legislature responded by passing SB 1386 in September.

Who must comply with SB 1386?



The law applies to any person or company that conducts business in California and owns or maintains computerized personal information. The law does not define what "conducting business in California" means. As a result, many companies not based in California may be affected by the law.

The data covered by the law is fairly narrow. Essentially, it covers people's last names and first names or initial, when the name is combined with Social Security numbers, drivers' license numbers or credit card or debit card numbers with passwords. Only information that falls under the law.

The law defines a breach as the unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information of California residents. "If a Nevada resident's information is compromised, then the disclosure requirement is not triggered," Pink said.

Once a breach has been discovered, the affected company has to notify California residents quickly. The law does not mandate a 24 or 48 hour notification. Notification can be delayed if the breach is reported to law enforcement and the authorities believe disclosure would hamper an investigation. Also, companies can hold off on disclosing the compromise in order to fix the security hole and restore the integrity of their systems, Pink said.

How to notify affected parties of a breach

Companies have some leeway as to how they notify affected people of a breach. Sending out a letter is one way, but that method is expensive. E-mail notification is considered OK, as long as the messages comply with the federal e-Sign Law.

Public notification is a third route for companies that suffer large breaches, but it's not "appetizing for companies, particularly if they are concerned about protecting their reputations," Pink said.

This route is open to companies for which notifying affected people would cost more than \$250,000, or if more than 500,000 people are affected. Public notification can also be done if a company does not have sufficient contact information for affected parties. A company has to e-mail the people they do have information for, post a "conspicuous notice" on its Web site and notify major statewide media of the breach.

Companies that don't comply with the law could face civil litigation from affected parties. "There is no end to [the] creativity of attorneys," Pink said.

Unresolved issues

There are still some questions about SB 1386. For example, it's unclear whether California can impose requirements on companies operating in the state. It could be interpreted that such a law affects interstate commerce, which the Constitution only allows Congress to regulate.

Encrypting personal data would exempt companies from the law, but there are no minimums on the strength of the encryption. "Does a company use encryption that can be unscrambled by anyone?" Pink said.

There are also some questions about what would happen if a low-level employee sees a breach and forgets to tell management. "Would the employee be held liable?"

Regardless of the questions raised by the law, companies still need to prepare to comply with it. Pink recommends that companies review their security systems and policies. Do they have personal information about California residents? Is that data encrypted, or can it be? Is such information accessible from the outside world?

Companies also need to establish procedures for dealing with local law enforcement. Educating employees about the law is also important, Pink said.

There has been some talk that Sen. Dianne Feinstein (D-Calif.) may introduce a similar law at the federal level, but such a proposal would face a lot of industry opposition. Other states may consider laws similar to California's, but many will likely "wait and see how the law works in practice," Pink said.

FOR MORE INFORMATION:

[SearchSecurity.com news exclusive: "Should you keep security holes secret?"](#)

[SearchSecurity.com technical tip: "Compliance with California's new mandatory disclosure law"](#)

[Best Web Links on standards and guidelines](#)

FEEDBACK: What is your enterprise's biggest concern regarding SB 1386?
Send your feedback to the [SearchSecurity.com news team](#).

SECURITY RELATED LINKS

Ads by Google

GLBA Security Compliance

Complete GLBA compliance solutions from assessment through remediation
www.metasecuritygroup.com

Security Awareness

Information security training for all employees. Free Demo.
www.inspiredelearning.com

Gramm-Leach-Bliley

Comply with Gramm-Leach-Bliley through document security
www.smartsoftkey.com

Backup, Archive & Restore

Protect your data with Storage Solutions from Quantum
www.quantum.com

Check Point Security

Intelligent Security Solutions 100% Compliance Security Here
CheckPoint.com

EMAIL A FRIEND

[Send the article you've just read to a friend](#)

LATEST HEADLINES

- >> [BREAKING NEWS: Expect nine Windows patches, some critical \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [Advanced vulnerability management: Best tools and tactics for enhanced security \(SearchSecurity.com\)](#)
- >> [Security Bytes: New malware making the rounds \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [Compressed files strike another blow to AV \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [Open source: Time to pay up \(SearchSecurity.com\) EXCLUSIVE!](#)

WHAT'S NEW

on SearchSecurity

- * [MESSAGE TO OUR READERS](#)
- * [Info Security Decisions May](#)
- * [Securing High Performance](#)
- * [Security School - Free Train](#)

TechTarget
Security Media



View this month's
issue and subscribe
today.

**INFORMATION
SECURITY
DECISIONS**

Apply online for free
conference admission.



[HOME](#)

[NEWS](#)

[TOPICS](#)

[IT KNOWLEDGE EXCHANGE](#)

[TIPS](#)

[ASK THE EXPERTS](#)

[WEBCASTS](#)

[WHITE PAPER](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Reprints](#)

SEARCH

SearchSecurity.com is part of the TechTarget network of industry-specific IT Web sites

[WINDOWS](#)

[ENTERPRISE IT MANAGEMENT](#)

[PLATFORMS](#)

SearchExchange.com
SearchVB.com
SearchWin2000.com
SearchWindowsSecurity.com
SearchWinSystems.com
Labmice.net
MyITForum.com

APPLICATIONS

SearchCRM.com
SearchSAP.com

SearchCIO.com
SearchDataCenter.com
SearchSMB.com

CORE TECHNOLOGIES

SearchDatabase.com
SearchEnterpriseVoice.com
SearchMobileComputing.com
SearchNetworking.com
SearchOracle.com
SearchSecurity.com
SearchStorage.com
SearchWebServices.com
WhatIs.com

Search390.com
Search400.com
SearchDomino.com
SearchEnterpriseLinux.com

TechTarget Expert Answer Center | TechTarget Enterprise IT Conferences | TechTarget Corporate Web Site | Media Kit

Explore **SearchTechTarget.com**, the guide to the TechTarget network of industry-specific IT Web sites.

All Rights Reserved, Copyright 2000 - 2005, TechTarget

Read our |

Explore the TechTarget Network at SearchTechTarget.com.

Activate your FREE member



The world's best security specific information news source for computer IT professionals



ADVERTISEMENT

you're loads

For bad guys, it means

HOME
NEWS
TOPICS
ITKNOWLEDGE EXCHANGE
TIPS
ASK THE EXPERTS
WEBCASTS
WHITE PAPER

SEARCH this site and the web

ADVANCED SEARCH | SITE MAP

ADVERTISEMENT

Stay secure with the world's most trusted source for unbiased security expertise. Get your free subscription to Information Security today!

[Home](#) > [News](#) > Should you keep...

[EMAIL THIS](#)

Security News:

Search for: in ALL NEWS Full TargetSearch with Google

Should you keep security holes secret?

By Michael S. Mimoso, News Editor
10 Jul 2002 | SearchSecurity

SITE SPONSOR

Unbiased expertise
for IT security pros

IT has had its fill of buggy software, and it's not going to wait 30 days any more to disclose what it knows.

At least, that's the overwhelming majority of the reaction from SearchSecurity users who recently commented on the full disclosure debate.

Close to two months ago, bug finder David Litchfield, who has a history of scrounging up buffer overflows in Microsoft, Oracle and Lotus software, said he had tired of lagging vendor response to his findings. No longer would he wait 30 days to disclose his discoveries, as the commonly accepted industry protocol suggests. Instead, he announced that he's giving vendors one week before he lets the world know about a software flub via his Vendor Notification Alert. Litchfield conceded he would not publicize details on any vulnerability, but that he would make the flub public along with any workarounds.

FOR MORE INFORMATION:

[More user comments on full disclosure](#)

[SearchSecurity news exclusive: "The disclosure debate rages"](#)

Feedback on this story? Send your comments to News Editor [Michael S. Mimoso](#)

SearchSecurity users responded to the firestorm with rousing support.

"I wouldn't even wait a week. There is no excuse for releasing bad code in the first place. If they had done the job right and had included security in the process from the beginning, there would be a lot fewer bugs to disclose," said Carrie L. Barrett, a developer with Delphi Corp., a Michigan-based mobile electronics and transportation components and system technology developer. "As a security developer, it is extremely frustrating. I have been fighting with developers for a long time over just this issue. My bottom line? Blow the whistle without waiting."

The other side of this debate, however, suggest that immediate disclosure of vulnerability details only arms crackers waiting to steal

corporate assets or damage reputations.

"I think Mr. Litchfield's approach shows a lot of immaturity. I believe that companies should be given as much

time as needed to issue a patch," said David A. Jacot. "Some security patches take more than a week just to fix, and I've even seen a programmer go in and fix a security problem only to find other issues which take time to solve."

Vulnerabilities cost enterprises worldwide billions of dollars. Nimda and Code Red, which exploited holes in Microsoft Internet Information Server (IIS) software, resulted in \$2.4 billion in losses.

"As long as vendors continue to act as if the problem isn't the security hole, but our knowing about the security hole, full public disclosure is the only protection the rest of us have," said Todd Knarr, a software developer. "If customers don't know about the holes, they can't put pressure on the vendors to fix them. No pressure means the vendor has no incentive. If the vendor won't take the initiative, full disclosure is the only way the customers find out they need to turn up the heat on the vendor."

Analyst firm Hurwitz Group recently tackled the issue in a survey of its clients, many of whom (44%) said that full disclosure is the only way to force companies into writing secure code. Sixty-seven percent said that immediate disclosure or less than a week is a reasonable amount of time from discovery to disclosure. Senior management members who responded, however, said that disclosure only serves to arm crackers trying to break into their systems to steal data.

Some SearchSecurity users may be willing to take that risk.

"Though I do agree that this could give hackers some early information that could lead to potential damage, I feel that in the long run the IT industry would be much better off by finally forcing software vendors to produce safer and more efficient products," said Nicholas Dippold, an administrator with RKA Petroleum of Romulus, Michigan. "It would be nice to actually purchase a product that lives up to it's expectations and offers the end user piece of mind that the product of choice will be safe right out of the box."

Vendors, SearchSecurity users said, are driven by the need to rush products out the door and often get to fixes in subsequent versions.

"It seems too many software vendors are so consumed by the all-mighty dollar that they are flooding the market with 'buggy' software by the droves and getting away with it! In my industry as well as most, if I put a product on the market that is shoddy at best, I'm going to take a tremendous hit for it," Dippold said. "However it seems our software friends live by a different set of rules, and as an admin, I for one am tired of taking the hits for the vendors mistakes!"

Some users compare software vendors to government when it comes to vulnerable products.

"Unless a company faces a major incident, there will be no impetus for security," said a SearchSecurity member who identified themselves as HC. "Vendors are not inclined to commit resources to clean up a mess in their code/products unless the threat is very, very real."

SECURITY RELATED LINKS

Ads by Google

Vulnerability Assessment

Accurate. Easy to use. No software required. Free QualysGuard trial.
www.Qualys.com

Vulnerability Assessment

Secures network, continuous audit w/ real-time reporting. Free Trial!
www.lockdownnetworks.com

Network Security Auditing

Network vulnerability assessment, penetrating testing, auditing.
www.sses.net

Vulnerability Management

Free 30-day Trial: Vulnerability & Compliance Management On-demand
www.TBDnetworks.com

Click
for a
subs



Full Threat Assessments

Experienced certified professionals protecting data and communications.

www.TotemSecurity.com**EMAIL A FRIEND**

Send the article you've just read to a friend

LATEST HEADLINES

- >> [RSA 2005: Raising the bar? \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [Desktop Summit '05: Time to turn Linux enthusiasts into evangelists \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [Critical flaw affects F-Secure products \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [RSA 2005: A chat with Harris Miller \(SearchSecurity.com\) EXCLUSIVE!](#)
- >> [How will Bill Gates' antivirus cliffhanger play out? \(SearchSecurity.com\)](#)

**WHAT'S NEW**

on SearchSecurity

- * [MESSAGE TO OUR READERS](#)
- * [Info Security Decisions May](#)
- * [Securing High Performance](#)
- * [Security School - Free Train](#)

TechTarget
Security MediaView this month's
issue and subscribe
today.**INFORMATION
SECURITY
DECISIONS**Apply online for free
conference admission.**HOME****NEWS****TOPICS****IT KNOWLEDGE EXCHANGE****TIPS****ASK THE EXPERTS****WEBCASTS****WHITE PAPER**[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Reprints](#)**SEARCH**

SearchSecurity.com is part of the TechTarget network of industry-specific IT Web sites

WINDOWS

[SearchExchange.com](#)
[SearchVB.com](#)
[SearchWin2000.com](#)
[SearchWindowsSecurity.com](#)
[SearchWinSystems.com](#)
[Labmice.net](#)
[MyITForum.com](#)

APPLICATIONS

[SearchCRM.com](#)
[SearchSAP.com](#)

ENTERPRISE IT MANAGEMENT

[SearchCIO.com](#)
[SearchDataCenter.com](#)
[SearchSMB.com](#)

CORE TECHNOLOGIES

[SearchDatabase.com](#)
[SearchEnterpriseVoice.com](#)
[SearchMobileComputing.com](#)
[SearchNetworking.com](#)
[SearchOracle.com](#)
[SearchSecurity.com](#)
[SearchStorage.com](#)
[SearchWebServices.com](#)
[WhatIs.com](#)

PLATFORMS

[Search390.com](#)
[Search400.com](#)
[SearchDomino.com](#)
[SearchEnterpriseLinux.com](#)

[TechTarget Expert Answer Center](#) | [TechTarget Enterprise IT Conferences](#) | [TechTarget Corporate Web Site](#) | [Media Kit](#)Explore [SearchTechTarget.com](#), the guide to the TechTarget network of industry-specific IT Web sites.

All Rights Reserved, Copyright 2000 - 2005, TechTarget

[Read our I](#)

The security you need, the protection you want.

WatchGuard Firebox SOHO 6tc
Compact, high-performance...



CDW

Explore the TechTarget Network at SearchTechTarget.com.

Activate your FREE member



The world's most security specific information resource for independent IT professionals



VeriSign® SSL Services.
Get a FREE SSL Security Kit.

[learn more >>](#)



[HOME](#) | [NEWS](#) | [TOPICS](#) | [ITKNOWLEDGE EXCHANGE](#) | [TIPS](#) | [ASK THE EXPERTS](#) | [WEBCASTS](#) | [WHITE PAPER](#)

SEARCH this site and the web

SEARCH

[ADVANCED SEARCH](#) | [SITE MAP](#)

Search Po

ADVERTISEMENT



Stay secure with the world's most trusted source for unbiased security expertise. Get your free subscription to Information Security today!

[Home](#) > [Tips](#) > [Guest Commentary](#) > Compliance with...

[EMAIL THIS](#)

Security Tips:

TIPS & NEWSLETTERS TOPICS

Search for: in [All Tips](#) [Full TargetSearch with Google](#)

GUEST COMMENTARY

Compliance with California's new mandatory disclosure law, part two: Strategies for compliance

Marc J. Zwillinger, chair of the Information Security and Anti-Piracy practice group, Sonnenschein Nath & Rosenthal

20 May 2003

Rating: -5.00- (out of 5)



This column is continued from part one of Compliance with California's new mandatory disclosure law.

Strategies for Compliance

Identify key systems containing personal information, and activate and enhance logging capabilities on such systems and/or deploy new technology designed to provide more forensic detail about conduct on networks. The statute is triggered when an entity knows or reasonably believes that unencrypted personal information of a California resident has been compromised. Unfortunately, the statute provides no guidance or examples to help determine what set of facts would give rise to a "reasonable belief" of an unauthorized acquisition of personal information. Therefore, corporations should first consider whether they have individual systems upon which the following information is stored in combination with a person's name: (1) social security number, (2) driver's license number or California ID card number or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account.

EXPLORE THIS AREA: RICH-MEDIA AD

Unbiased expertise
for IT security

INFORMATION
SECURITY

If there are systems that contain such information, any intrusion into such systems (or combination of systems from which the pieced together) should be examined to determine if the intruder was able to obtain access to the files containing such information. If the intruder actually obtained the information (i.e., downloaded the files or stole the hard drive from the computers), the California statute triggered. If the intruder obtained root access to the system containing relevant files, but there is no way to determine whether accessed, a conservative approach requires acting as if the statute had been triggered. In such cases, immediate and detailed examination may be critical to taking a more aggressive approach, because the results of such examination could rule out the

information. Storing either the individual's name or the relevant personal information in encrypted form would also obviate the

Prospectively, a company should consider employing measures to make more reliable the determination of whether personal information has been acquired by an unauthorized person. In addition to developing systems to track network access, existing activity and capabilities can be turned up to their maximum settings and maintained remotely (on a system other than the one being logged) to ensure secure detailed recordation of activities on computers and systems that store or process unencrypted personal information. (For the tweaks necessary to enhance the security and comprehensiveness of logging and passive network surveillance, see, e.g., "Incident Response: Investigating Computer Crime," pp. 39-50, 198-222.) In addition, now that encryption technology has become seamlessly integrated into standard applications, the time may be ripe to revisit the ideas of storing data in encrypted form.

Amend incident response plan to require notification of counsel's office or incident response team when breach of key information has been detected. Because a company will likely be deemed to have been on notice when an intrusion or unauthorized use of the information has been detected by individuals in the information security or IT department, it is important that corporations ensure that their incident response plans that provide for timely reporting of incidents to a person or group responsible for making notification decisions.

Adopt or revise corporate incident response policies to provide a notification plan (at least California residents) on terms more flexible than the substitute notice provisions of Section §1798.82(g)(3). The two key exceptions to the formal statutory notice requirements are: (1) where "a person or business maintains its own notification procedures as part of an information security plan that provides for the treatment of personal information and is otherwise consistent with the timing requirements of this part... if the person or business maintains its policies in accordance with its policies in the event of a breach of security of the system," and (2) where a law enforcement agency determines that notification will impede a criminal investigation.

The first exception is the most useful in avoiding the strict notification regime of the California statute, because the California statute allows latitude to those companies that have an organizational incident response plan that includes some form of notification to customers. The statute must still comport with the timing requirements of the statute, which requires notice within "the most expedient time possible and without unreasonable delay, consistent with legitimate needs of law enforcement . . . or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system." (Although the statute does not provide any specific time period for providing notice, the incident that sparked the legislation involved the failure of a California state agency to notify state employees of a large-scale breach of information for more than two weeks after the breach was discovered.) Nevertheless, an internal plan provides far more flexibility and scope of the notice and more certainty with regard to timing issues. For example, the thresholds for providing "substitute notice" under the California statute are quite high -- before substitute notice can be invoked, the costs of providing direct notice must exceed \$250,000, more than 500,000 people must be affected by the incident. Even when invoked, the substitute notice provisions are onerous, requiring direct notice by mail and Web site posting and notification to major statewide media.

If a corporation adopts its own notification procedures as part of an information security plan, however, it can set its own thresholds for when direct notice is required. Similarly, a corporation's substitute notice plan need not involve all three mandatory aspects of the California statute. According to the statute, the only requirement placed on a corporation's own notification plan is that it comport with the timing requirements of the statute.


Amend or draft incident response plan to contain mandatory period for investigation and remediation before decision to notify third-party notifications. An internal notification plan may provide additional flexibility because such a plan can contain a defined pre-notification investigation and remediation period to "determine the scope of the breach and restore the reasonable integrity of the data system." Such a mandatory pre-reporting period is advisable regardless of the California statute as it provides time for the company to determine the nature and extent of any unauthorized activity so that the company can make informed and thoughtful decisions on (1) the scope of necessary forensic examination; (2) the nature of remediation efforts; (3) the need to notify customers, shareholders, and other third-parties; and (4) the desirability of making a law enforcement referral or pursuing civil enforcement and recovery. While the pre-reporting period may vary depending on the nature of the suspected unauthorized activity, setting a minimum time period for evaluation will allow the corporation to pause for informed decision-making before committing to the irreversible step of notification.


Where notice is ultimately required, either by a corporation's own plan or by operation of California law, a corporation seeking to avoid notice may be able to defer notice at the request of a law enforcement agency. Although the investigating agency must first make a determination that the notification would interfere with the criminal investigation, many law enforcement agencies frequently provide such deferrals in computer intrusion cases, and the agency's standard operating procedures should be ascertainable through a pre-referral conference with the agency.

Review all third-party contracts involving the transfer of sensitive personal data to ensure that such contracts contain security provisions, including mandatory notification, rights to investigate, and right to participate in or control reporting of breaches involving customer data. The California law applies to all businesses that own or license computerized data. The statute provides an exception for circumstances where the owned or licensed data is in the possession or control of a third-party or subcontractor who is not a subcontractor for unauthorized acquisition. Accordingly, corporations should take measures to ensure that outsourcing contracts -- in addition to representations and warranties regarding information security issues (Such provisions are required in certain instances by the Sarbanes-Oxley Act and its implementing regulations.) -- also contain provisions requiring mandatory notification of suspected breaches, and the corporation to participate in the investigation into such incidents and to potentially control any decisions with regard to external

DISCLAIMER: Our Tips Exchange is a forum for you to share technical advice and expertise with your peers and to learn from other enterprise professionals. TechTarget provides the infrastructure to facilitate this sharing of information. However, we cannot guarantee the accuracy of material submitted. You agree that your use of the Ask The Expert services and your reliance on any questions, answers, information or advice received through this Web site is at your own risk.

Do you like this tip? [Email](#) your opinion or rate the tip:

 **Rate this Tip:** In order to rate this tip, you must be a registered member of [searchSecurity.com](#)

 **Register now** to start rating these tips

Already a member? [Log In](#)

 **Free tips via email**

LATEST TIPS & NEWSLETTERS

- >> [Honeypots can strengthen reconnaissance and lower intrusion noise](#)
- >> [How permanent is your storage solution?](#)
- >> [Freedom of speech or lack of professional responsibility?](#)
- >> [Computer Security Institute's leader responds to Abagnale flap](#)
- >> [This year compliance, next year control](#)

WHAT'S NEW

on [searchSecurity](#)

1. [RSA Security Coverage](#)
2. [Info Security Decisions May '05](#)
3. [Subscribe to Info Security Mag](#)
4. [Free Security Book Chapter Download](#)

SECURITY RELATED LINKS

Ads by Google

[GLBA Security Compliance](#)

Complete GLBA compliance solutions from assessment through remediation
[www.metasecuritygroup.com](#)

[USA Patriot Act Solutions](#)

Complete tracking and reporting for Patriot Act Section 326. Free Trial
[www.usapatriotactcompliance.com](#)

[GLBA Security Compliance](#)

Award-winning network auditing and vulnerability mgmt. Try QualysGuard
[www.Qualys.com](#)

[Free Compliance Guide](#)

The Facts On Patriot Act Section 326 Compliance: Free Download
[www.innovativesystems.com](#)

[HIPAA Compliance](#)

with LT Auditor. Free White Paper covers compliance through auditing.
[www.bluelance.com](#)

TechTarget
Security Media



View this month's
issue and subscribe
today.

**INFORMATION
SECURITY
DECISIONS**

Apply online for free
conference admission.



[HOME](#) | [NEWS](#) | [TOPICS](#) | [IT KNOWLEDGE EXCHANGE](#) | [TIPS](#) | [ASK THE EXPERTS](#) | [WEBCASTS](#) | [WHITE PAPER](#)

[About Us](#) | [Contact Us](#) | [For Advertisers](#) | [For Business Partners](#) | [Reprints](#)

SEARCH

SearchSecurity.com is part of the TechTarget network of industry-specific IT Web sites

WINDOWS
[SearchExchange.com](#)

ENTERPRISE IT MANAGEMENT
[SearchCIO.com](#)

PLATFORMS
[Search390.com](#)

SearchVB.com
SearchWin2000.com
SearchWindowsSecurity.com
SearchWinSystems.com
Labmice.net
MyITForum.com

APPLICATIONS

SearchCRM.com
SearchSAP.com

SearchDataCenter.com
SearchSMB.com

CORE TECHNOLOGIES

SearchDatabase.com
SearchEnterpriseVoice.com
SearchMobileComputing.com
SearchNetworking.com
SearchOracle.com
SearchSecurity.com
SearchStorage.com
SearchWebServices.com
WhatIs.com

Search400.com
SearchDomino.com
SearchEnterpriseLinux.com

TechTarget Expert Answer Center | TechTarget Enterprise IT Conferences | TechTarget Corporate Web Site | Media Kit

Explore **SearchTechTarget.com**, the guide to the TechTarget network of industry-specific IT Web sites.

All Rights Reserved, Copyright 2000 - 2005, TechTarget

Read our |

BILL NUMBER: SB 1386 CHAPTERED
BILL TEXT

CHAPTER 915

FILED WITH SECRETARY OF STATE SEPTEMBER 26, 2002

APPROVED BY GOVERNOR SEPTEMBER 25, 2002

PASSED THE SENATE AUGUST 30, 2002

PASSED THE ASSEMBLY AUGUST 26, 2002

AMENDED IN ASSEMBLY AUGUST 23, 2002

AMENDED IN ASSEMBLY AUGUST 5, 2002

AMENDED IN ASSEMBLY JULY 25, 2002

AMENDED IN ASSEMBLY JUNE 30, 2002

AMENDED IN ASSEMBLY JUNE 20, 2002

AMENDED IN ASSEMBLY JUNE 6, 2002

AMENDED IN SENATE MARCH 20, 2002

INTRODUCED BY Senator Peace
(Principal coauthor: Assembly Member Simitian)

FEBRUARY 12, 2002

An act to amend, renumber, and add Section 1798.82 of, and to add Section 1798.29 to, the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 1386, Peace. Personal information: privacy.

Existing law regulates the maintenance and dissemination of personal information by state agencies, as defined, and requires each agency to keep an accurate account of disclosures made pursuant to specified provisions. Existing law also requires a business, as defined, to take all reasonable steps to destroy a customer's records that contain personal information when the business will no longer retain those records. Existing law provides civil remedies for violations of these provisions.

This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The bill would permit the notifications required by its provisions to be delayed if a law enforcement agency determines that it would impede a criminal investigation. The bill would require an agency, person, or business that maintains computerized data that includes personal information owned by another to notify the owner or licensee of the information of any breach of security of the data, as specified. The bill would state the intent of the Legislature to preempt all local regulation of the subject matter of the bill. This bill would also make a statement of legislative findings and declarations regarding privacy and financial security.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. (a) The privacy and financial security of individuals

is increasingly at risk due to the ever more widespread collection of personal information by both the private and public sector.

(b) Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Internet Web sites are all sources of personal information and form the source material for identity thieves.

(c) Identity theft is one of the fastest growing crimes committed in California. Criminals who steal personal information such as social security numbers use the information to open credit card accounts, write bad checks, buy cars, and commit other financial crimes with other people's identities. The Los Angeles County Sheriff's Department reports that the 1,932 identity theft cases it received in the year 2000 represented a 108 percent increase over the previous year's caseload.

(d) Identity theft is costly to the marketplace and to consumers.

(e) According to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative.

SEC. 2. Section 1798.29 is added to the Civil Code, to read:

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would

permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 3. Section 1798.82 of the Civil Code is amended and renumbered to read:

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.

(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

SEC. 4. Section 1798.82 is added to the Civil Code, to read:

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section

shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

SEC. 5. This act shall become operative on July 1, 2003.

SEC. 6. This act deals with subject matter that is of statewide concern, and it is the intent of the Legislature that this act supersede and preempt all rules, regulations, codes, statutes, or ordinances or all cities, counties, cities and counties, municipalities, and other local agencies regarding the matters expressly set forth in this act.